

Docket No. 200314912-1  
Application No.: 10/827,218

### **Remarks**

This communication is responsive to the Office Action of July 18, 2008. Reexamination and reconsideration of claims is respectfully requested.

### **Summary of The Office Action**

Claims 1, 4-5, 7-18, and 45-46 were rejected under 35 U.S.C. 102(e) as being anticipated by Challenger (US Patent No. 7,281,010).

Claims 2, 3, 6 were rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger (US Patent No. 7,281,010) in view of Ranganathan (US Pub. No. 20050138423).

Claims 1-18 and 45-46 were elected.

### **The Present Amendments**

Claim 1 has been amended. The amendments are supported by, for example, language from claim 8, or the specification page 8, lines 3-4. These sections also support the amendments to claim 6 and 45. Thus no new matter has been added.

Dependent claim 5 has been rewritten into independent form including all elements from parent claim 1. The scope of claim 5 has not changed.

New claim 48 depends from claim 45. It is supported by, for example, the specification page 17, lines 23-27. Thus no new matter has been added.

New claim 49 depends from claim 45. It is supported by, for example, the specification page 8, lines 25-26. Thus no new matter has been added.

Docket No. 200314912-1  
Application No.: 10/827,218

Claims 19-44 and 47 are canceled as being non-elected claims. The inventorship of the application does not change due to the cancellation of claims. Thus an amendment of inventorship is not required.

**I. Claims 1, 4-5, 7-18, and 45-46 were rejected under 35 U.S.C. 102(e) as being anticipated by Challenger (US Patent No. 7,281,010).**

Independent Claim 1

Claim 1 recites:

where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform;

Challenger fails to teach or suggest this feature. Rather, Challenger discloses:

The present invention, however, makes use of the ability of a TPM to have non-migratable keys as well as migratable keys. Migratable keys can be transferred to other TPMs, and non-migratable keys cannot be transferred. Thus, such non-migratable keys are locked to the hardware, i.e., the TPM 951. With such non-migratable keys, the TPM 951 can only decrypt such keys.

(Challenger, col. 3, lines 54-61) [emphasis added]

Challenger further discloses that "the migration of 2048-bit RSA multi-prime keys, ECC keys, or any equivalent are not permitted under the TCPA specification." (col. 3, lines 11-13). Challenger describes its storage root key as "a private, 2048 bit RSA key" (col. 3, lines 19-20) and thus is a non-migratable key.

Therefore, Challenger fails to teach or suggest the claimed logic that performs cryptographic key maintenance including migrating a non-migratable storage root key as recited in claim 1. Claim 1 patentably distinguishes over the references of record and should now be in condition for allowance.

Docket No. 200314912-1  
Application No.: 10/827,218

**Independent Claim 5**

Claim 5 was rejected based on Challenger column 4, lines 5-22. This section discusses loading trees of keys. There is no discussion or suggestion of USB (universal serial bus) tokens or that a system as claimed is part of a USB token. Therefore, Challenger fails to teach claim 5 and a prima facie rejection has not been established. The rejection is improper and should be withdrawn.

**Dependent Claim 6**

Claim 6 depends from independent claim 5 and recites that "the logic is configured to migrate one or more non-migratable keys from a trusted platform module associated with the trusted platform and configured to use the migrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module."

Challenger fails to teach or suggest migrating non-migratable keys and fails to teach or suggest having a different component be able to decrypt items that were encrypted by the trusted platform module. Rather, Challenger discloses that non-migratable keys cannot be transferred and that only the trusted platform module TPM can decrypt its own keys (Challenger, col. 3, lines 54-61).

Therefore, Challenger fails to teach or suggest claim 6. Claim 6 patentably distinguishes over the references of record and should now be in condition for allowance.

**Independent Claim 45**

Claim 45 recites a system comprising a trusted platform module and a subordinate trusted platform module. The references fail to teach or suggest such a system. Furthermore, claim 45 recites that the subordinate trusted platform module includes logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module. As previously

Docket No. 200314912-1  
Application No.: 10/827,218

discussed, Challenger fails to teach or suggest such a feature. Instead, Challenger only discloses that non-migratable keys cannot be transferred. Challenger fails to support a prima facie rejection. The rejection is improper and should be withdrawn.

**Dependent Claim 17**

Claim 17 was rejected based on Challenger column 3, lines 47-67. This section discusses migratable and non-migratable keys. There is no discussion or suggestion of binding a logic to the trusted platform in a one-to-one manner as recited. Therefore, Challenger fails to teach claim 17 and a prima facie rejection has not been established. The rejection is improper and should be withdrawn.

**II. Claims 2, 3, 6 were rejected under 35 U.S.C. 103(a) as being unpatentable over Challenger (US Patent No. 7,281,010) in view of Ranganathan (US Pub. No. 20050138423).**

These claims depend from independent claim 1. As shown above, Challenger fails to teach or suggest claim 1 and thus fails to support a prima facie rejection for its dependent claims. The rejection should be withdrawn.

FROM

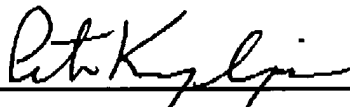
(MON) OCT 20 2008 14:16/ST. 14:13/NO. 6302335356 P 12

Docket No. 200314912-1  
Application No.: 10/827,218

**Conclusion**

For the reasons set forth above, the claims are now in condition for allowance.  
An early allowance of the claims is earnestly solicited.

Respectfully submitted,



---

Peter Kraguljac (Reg. No. 38,520)

(216) 503-5500

Kraguljac & Kalnay, LLC  
4700 Rockside Road  
Summit One, Suite 510  
Independence, OH 44131